UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/069,118	06/11/2002	Masayuki Hatanaka	020234	3335

38834 7590 04/28/2006

WESTERMAN, HATTORI, DANIELS & ADRIAN, LLP
1250 CONNECTICUT AVENUE, NW
SUITE 700
WASHINGTON, DC 20036

EXAMINER	
CHEN, SHIN HON	
ART UNIT	PAPER NUMBER
2131	

DATE MAILED: 04/28/2006

Please find below and/or attached an Office communication concerning this application or proceeding.

Office Action Summary	Application No. 10/069,118	Applicant(s) HATANAKA ET AL.
	Examiner Shin-Hon Chen	Art Unit 2131

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on 29 March 2006.

2a)□ This action is **FINAL**. 2b)☒ This action is non-final.

3)□ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) 23-63 is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)□ Claim(s) _____ is/are allowed.

6)☒ Claim(s) 23-63 is/are rejected.

7)□ Claim(s) _____ is/are objected to.

8)□ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)□ The specification is objected to by the Examiner.

10)☒ The drawing(s) filed on 11 June 2002 is/are: a)☒ accepted or b)□ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)□ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☒ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☒ All b)□ Some * c)□ None of:

1.☒ Certified copies of the priority documents have been received.

2.□ Certified copies of the priority documents have been received in Application No. _____.

3.□ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) □ Notice of References Cited (PTO-892)
2) □ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) □ Information Disclosure Statement(s) (PTO-1449 or PTO/SB/08)
Paper No(s)/Mail Date _____.
4) □ Interview Summary (PTO-413)
Paper No(s)/Mail Date. _____ .
5) □ Notice of Informal Patent Application (PTO-152)
6) □ Other: _____.

DETAILED ACTION

1. Claims 23-63 are examined.

Continued Examination Under 37 CFR 1.114

2. A request for continued examination under 37 CFR 1.114, including the fee set forth in 37 CFR 1.17(e), was filed in this application after final rejection. Since this application is eligible for continued examination under 37 CFR 1.114, and the fee set forth in 37 CFR 1.17(e) has been timely paid, the finality of the previous Office action has been withdrawn pursuant to 37 CFR 1.114. Applicant's submission filed on 3/29/06 has been entered.

Response to Arguments

3. Applicant's remarks filed on 3/29/06 have been fully considered but they are not persuasive.

Regarding applicant's remarks, applicant has amended independent claims to expedite prosecution and further clarify the present invention. However, the claims are still not presented in a clearly understandable form and fail to particularly point out and distinctly claim the invention. For instance, the claims does not disclose 1) how the first decryption key is generated and obtained, 2) if the content key is encrypted with the first key, how is the session key able to decrypt the encrypted content? 3) the encrypted content key was already decrypted at a first decryption processing unit and why is there a need for a second decryption processing unit to extract the content key? Therefore, applicant is advised to revise the claims in better form.

For rejections of claims 23-63, please refer to the previous office action sent out on 6/16/05. Further explanations may be provided upon due course.

Claim Objections

4. Claims 23, 28, 34, 45 and 53 are objected to because of the following informalities: It is not clear to the examiner as to which portion of these claims is preamble and which potion is body of the claim. Appropriate correction is required.

5. Claims 23-63 are objected to for the following reason. The claim Language must be more specific for Examiner to understand and be able to search for the invention. The claims as presented cause massive ambiguities, which make examination highly difficult. Examiner will interpret the claims to their broadest reasonable interpretation until a more clear presentation of the claims has been displayed.

Claim Rejections - 35 USC § 112

6. The following is a quotation of the second paragraph of 35 U.S.C. 112:

> The specification shall conclude with one or more claims particularly pointing out and distinctly claiming the subject matter which the applicant regards as his invention.

7. Claims 23-63 are rejected under 35 U.S.C. 112, second paragraph, as being indefinite for failing to particularly point out and distinctly claim the subject matter which applicant regards as the invention.

Regarding claims 23, 28, 34, 45 and 53: it's not clear to the examiner what is the difference between the content key, decryption key, encryption key, session key and public key the terms are being used interchangeably which makes difficult for the examiner to identify the scope of the claim . Further more it's not clear to the examiner what the first and the second encryption units do in regards to encrypting the keys and the content as far as the claims go. Also it's not clear to the examiner what is the difference between the first session key and the second session key.

Regarding claims 26, 49 and 57: The claims recite using the private key to encrypt the session key and then the claim recites using the public key to encrypt the session key. It's not clear to the examiner which key is used to encrypt the session key and where the session key is being encrypted.

Regarding claims 31, 37 and 43: it's not clear to the examiner which session key is used to obtain the content key or the decryption key.

Regarding claims 33, 35, 44, 46 and 54: it's not clear to the examiner what is meant by authentication key or if the authentication key is being used interchangeably with public private key.

Regarding claims 37 and 43: it's not clear to the examiner what's the difference between the unique decryption key in claim 12 and the second decryption key in claims 15 and 21.

Claims not specifically mentioned are rejected on virtue of their dependency on claims 23, 28, 34, 45 and 53

The claim Language must be more specific for Examiner to understand and be able to search for the invention. The claims as presented cause massive ambiguities, which make examination highly difficult. Examiner will interpret the claims to their broadest reasonable interpretation until a more clear presentation of the claims has been displayed.

Claim Rejections - 35 USC § 102

8. The following is a quotation of the appropriate paragraphs of 35 U.S.C. 102 that form the basis for the rejections under this section made in this Office action:

> A person shall be entitled to a patent unless –
>
> (e) the invention was described in (1) an application for patent, published under section 122(b), by another filed in the United States before the invention by the applicant for patent or (2) a patent granted on an application for patent by another filed in the United States before the invention by the applicant for patent, except that an international application filed under the treaty defined in section 351(a) shall have the effects for purposes of this subsection of an application filed in the United States only if the international application designated the United States and was published under Article 21(2) of such treaty in the English language.

9. Claims 23-63 are rejected under 35 U.S.C. 102(e) as being anticipated by Ginter et al. US (5,917,912).

Regarding claims 23, 28, 34, 45 and 53: Ginter discloses a data reproduction apparatus (200) decrypting encrypted content data to reproduce content data, comprising:

A data reproduction unit (1500) to reproduce said encrypted content data (Col 55, lines 33-38 / Content creator) and a data storage unit (120) storing said encrypted content data (Col 62, lines 50-56) and an encrypted content key that is a content key directed to decrypt said encrypted content data in an encrypted form decrypt able with a first decryption key (Col 70, lines 58-67 and Col 71, lines 45-52) unique to said data reproduction unit (Col 202, line 60 through Col 203 line 9 / the key obtained through the certificate is used to encrypt the content), and providing said encrypted content data and said encrypted content key to said data reproduction unit, (Col 67, lines 38-55) wherein said data reproduction unit comprises:

A session key generation unit (1520) generating a session key updated at every access to obtain said content key with respect to said data storage unit, (Col 219, lines 19-25)

A first encryption processing unit (1540) encrypting said session key using a public encryption key that can be decrypted at said data storage unit and that is unique to said data storage unit, and providing said encrypted session key to said data storage unit, (Col 219, lines 41-47)

A first decryption-processing unit (1506) using said session key to decrypt said encrypted content key, that is an encrypted version of said content key using said session key, said encrypted content key formally obtained from said data storage unit, (Col 192, lines 13-25 and Col 219, lines 32-39)

A first key-hold unit (1540) pre-storing said first decryption key, (Col 71, lines 45-52 and Col 211, lines 1-28 / a table of keys being used by the system and the storage location)

A second decryption processing unit (1530) extracting said content key by applying a decryption process on an output from said first decryption processing unit using (Col 215, lines 2-8 and Col 192, lines 1-7) said first decryption key stored in said first key hold unit, (Col 211, lines 31-37) and a third decryption processing unit (1520) receiving said encrypted content data read out from said data storage unit to decrypt said encrypted content data using a content key (Col 192, lines 29-52) extracted by said second decryption processing unit to extract content data. (Col 191, lines 46-62)

Regarding claims 24, 29, 50, 51, 58 and 59: Ginter discloses the data reproduction apparatus according to claim 23, said content data being coded audio data coded according to a coding scheme to reduce an amount of data, (Col 65, lines 29-31) wherein said data reproduction unit comprises an audio decoding unit (1508) reproducing audio data based on said coding scheme from said coded audio data,(Col 68, lines 5-19) and
a digital-analog converter (1512) converting said reproduced audio data into an analog signal.(Col 62, lines 1-10)

Regarding claims 25, 30, 42, 52, 62 and 63: Ginter discloses the data reproduction apparatus according to claim 23, wherein said data reproduction unit is provided in a security region that cannot be read out by a third party. (Col 63, line 58 through Col 64, line 3 / Secure location and tamper resistant barrier)

Regarding claims 26, 49 and 57: Ginter discloses the data reproduction apparatus according to claim 23, wherein said data storage unit (120) comprises
a record unit (1412) to store data applied to said data storage unit, (Col 54, lines 23-58)

a second key hold unit (140 1) storing said public encryption key unique to said data storage unit (Col 202, line 60 through Col 203 line 9), and that can supply said public encryption key to said data reproduction unit,(Col 67, lines 38-55)

a third key hold unit (1402) storing a second decryption key used to decrypt data encrypted with said public encryption key, (Col 211, lines 48-56)

a fourth decryption processing unit (1404) using said second decryption key to decrypt said first session key transmitted from said data reproduction unit in an encrypted form by said public encryption key, (Col 162, lines 56-62 and Col 211, lines 38-47) and

a second encryption processing unit (1406) encrypting encrypted content key stored in said recording unit using said first session key extracted at said fourth decryption processing unit for output. (Col 209, lines 1-5 and Col 210, lines 18-32)

Regarding claims 27, 32, 36, 38 and 41: Ginter discloses the data reproduction apparatus according to claim 23, wherein said data storage unit is detachable with respect to said data reproduction unit. (Col 62, lines 26-32 and Col 231, lines 19-25)

Regarding claims 31, 47 and 43: Ginter discloses the data reproduction apparatus according to claim 28, wherein said data storage unit (130, 140) comprises a recording unit (1412) to store data applied to said data storage unit, (Col 54, lines 23-58)

a second session key generation unit (1450) generating said first session key, (Col 219, lines 19-25)

a second encryption processing unit (1452) applying an encryption process using a public encryption key unique to said data reproduction unit and directed to apply encryption that can be decrypted with said unique decryption key, (Col 162, lines 56-62 and Col 211, lines 38-47)
a fourth decryption processing unit (1454) using said first session key to decrypt said second session key transmitted from said data reproduction unit in an encrypted form with said first session key, (Col 215, lines 2-8 and Col 192, lines 1-7) and
a third encryption processing unit (1456) carrying out an encryption process by said first session key extracted at said fourth decryption processing unit for output, (Col 209, lines 1-5 and Col 210, lines 18-32) said content key stored in said recording unit being encrypted at said second encryption processing unit and further encrypted at said third encryption processing unit to be supplied to said data reproduction unit. (Col 219, lines 41-47)

Regarding claims 33 and 44: Ginter discloses the data reproduction apparatus according to claim 31, further comprising: an authentication data hold unit (1560) storing and supplying to said data storage unit authentication data unique to said data reproduction unit together with said public encryption key in an encrypted form decryptable by an authentication key at said data storage unit, (Col 96, 5-17 and Col 163, lines 31-43); wherein said data storage unit (140) comprises a fifth decryption processing unit (1460) decrypting and extracting said authentication data and said public encryption key applied from said data reproduction unit in an encrypted form by said authentication key, (Col 204, 13-29) and control means carrying out an authentication process to determine whether to output said content key to a data reproduction unit from which said authentication data is output based on said authentication data extracted by said fifth decryption processing unit. (Col 202, line 60 through Col 203, line 9)

Regarding claims 35, 46 and 54: Ginter discloses the data reproduction apparatus according to claim 34, further comprising an authentication data hold unit (1560) storing, in an encrypted form decryptable by an authentication key, (Col 96, 5-17 and Col 212, lines 34-49) a public encryption key that is an encryption key unique to said data reproduction unit and directed to apply encryption that is decryptable with said unique decryption key and authentication data unique to said data reproduction unit, (Col 163, lines 31-43 and Col 204, 13-29) and that can output the stored public encryption key and authentication data to said data storage unit. (Col 12, line 56 through Col 213 ,line 4)

Regarding claims 39 and 60: Ginter discloses the data reproduction apparatus according to claim 34, further comprising an interface for connection to a portable
telephone network. (Col 60, lines 26-30)

Regarding claims 40 and 61: Ginter discloses the data reproduction apparatus according to claim 39, further comprising a conversation processing unit to carry out conversation via said interface. (Col 60, lines 40-48 / connection device as a Modem)

Regarding claims 47 and 55 : Ginter discloses the data reproduction module according to claim 45, wherein said content key is input from an external source to said data reproduction module in an encrypted form with said second session key, (Col 213, lines 6-13 and Col 217, lines 50-58) and said second decryption processing unit (1556) provides a decrypted result to said third decryption processing unit (1520) as a content key directed to decrypt said encrypted content data. (Col 215, lines 2-13)

Regarding claims 48 and 56: Ginter discloses the data reproduction module according to claim 45, wherein said content key is input from an external source to said data reproduction module in an encrypted form decryptable with said first decryption key (Col 211, lines 31-55), and further encrypted with said second session key,(Col 219, lines 20-39) wherein said first decryption processing unit decrypts using said first decryption key a content key in an encrypted form decryptable with said first decryption key which is an output of said second decryption processing unit (1556) to extract and provide to said third decryption processing unit (1520) said content key. (Col 215, lines 2-21).

Conclusion

10. Any inquiry concerning this communication or earlier communications from the examiner should be directed to Shin-Hon Chen whose telephone number is (571) 272-3789. The examiner can normally be reached on Monday through Friday 8:30am to 5:30pm.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Ayaz Sheikh can be reached on (571) 272-3795. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free).

Shin-Hon Chen
Examiner
Art Unit 2131

SC

CHRISTOPHER REVAK
PRIMARY EXAMINER

4/26/06